INFORMATION ASSURANCE DIRECTORATE

“INFORMATION ASSURANCE LEADERSHIP FOR THE NATION”

FREQUENTLY ASKED QUESTIONS

NATIONAL POLICY REGARDING THE EVALUATION OF COMMERCIAL IA PRODUCTS

WHAT IS IT?

WHY IS IT IMPORTANT?

HOW THE PROCESS WORKS?

IMPORTANCE OF COMPLIANCE?

15 February 2002

SUBJECT: Frequently Asked Questions Regarding National Information Assurance (IA) Acquisition Policy (NSTISSP No. 11)

TO: IA Industry Leaders

During December of 2000, Mr. Art Money, the former Chairman of the National Security Telecommunications and Information Systems Security Committee (NSTISSC), sent out a memorandum (NSTISSC-068-00, SUBJECT: Implementation of National IA Acquisition Policy, dated 5 December 2000) that focused attention on the need for industry and government involvement with the requirements of NSTISSP No. 11, the National IA Acquisition Policy. As we draw closer to 1 July 2002, the date requiring full compliance with the requirements of the policy, it is clear that much confusion remains among the community of vendors of IA products about what NSTISSP No. 11 means, and what requirements it levies upon users and vendors. The purpose of this memorandum and its enclosure is to address and alleviate that confusion.

As the U.S. Government continues its migration from the exclusive use of Government Off-the-Shelf (GOTS) products to a mix of Commercial Off-the-Shelf (COTS) and GOTS products for the protection of our national security systems, it becomes critical that users of those systems have a means to validate that IA products provide the advertised security functionality. Therefore, NSTISSP 11 was promulgated for purposes of mandating the use of a standardized evaluation process that will provide confidence in the security offered in these products. The National Security Agency (NSA) and the National Institute of Standards and Technology (NIST) have implemented programs through the National Information Assurance Partnership (NIAP) and the NIST Cryptographic Module Validation Program (CMVP) to facilitate these evaluations.

I hope that this information is both informative and useful. Additional information on the NSA and NIST efforts to implement the requirements of NSTISSP No. 11 can be obtained from the web sites also listed at the end of the enclosure. The following organizations can also be contacted to answer any questions:

NIST: (301) 975-2941

NSA: (410) 854-4458

This correspondence and its enclosure will also be posted to the homepage of the National Security Agency (http://www.nsa.gov) and can be accessed by clicking on "INFOSEC."

MICHAEL J. JACOBS
Director
Information Assurance Directorate

NATIONAL INFORMATION ASSURANCE (IA) ACQUISITION POLICY REQUIREMENTS AND IMPLEMENTATION

Why is there a need for a national IA acquisition policy?

The technology advances and threats of the past decade have drastically changed thinking and approaches to protecting national security systems and information. The U.S. Government has migrated from the exclusive use of Government Off-the-Shelf (GOTS) products to a mix of Commercial Off-the-Shelf (COTS) and GOTS products for the protection of information within our national security systems. The proliferation of COTS information assurance (IA) products[1] such as firewalls and Intrusion Detection Systems, as well as IA-enabled products[2] such as operating systems and database management systems with security attributes, has provided the community of users with a multitude of security products to choose from. All of these products come with their own specific claims relative to the security robustness[3] they provide. In this context, it is important that COTS IA and IA-enabled products acquired by U.S. Government Departments and Agencies be subject to a standardized evaluation process that will provide some validation that these products perform as advertised.

What is the objective of NSTISSP No. 11?

The objective of NSTISSP No. 11 is to ensure that COTS IA and IA-enabled products acquired by the U.S. Government for use in national security systems perform as advertised by their respective manufacturers, or satisfy the security requirements of the intended user. To achieve this objective, the policy requires that COTS products be evaluated and validated in accordance with either the International Common Criteria for Information Technology Security Evaluation, or the National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 140-2. Supportive

---

[1] An *IA product* is an IT product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control and non-repudiation of data); correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls and intrusion detection devices.

[2] An *IA-enabled product* is a product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems.

[3] *Security Robustness* is determined by security functionality (e.g., encryption), plus the strength of the implementing mechanism (e.g., 256 bit key length), plus security assurance (achieved through testing, evaluation, etc.).

of the intent and implementation of NSTISSP No. 11, the National Security Agency (NSA) and NIST have collaborated to establish the following two evaluation and validation programs:

- The National Information Assurance Partnership **(NIAP)**'s Common Criteria Evaluation and Validation Scheme **(CCEVS)** Program; and
- The NIST's Federal Information Processing Standard **(FIPS)** Cryptographic Module Validation Program **(CMVP).**

What is the NIAP CCEVS?

The NIAP CCEVS Program (hereinafter referred to as the NIAP Program) is a collaborative effort between NIST and NSA designed to meet the security evaluation needs of both IT/IA producers and users. The program fosters the availability of standardized specifications and testing methods for evaluating the security robustness of COTS IA and IA-enabled products. Additionally, it is designed to foster the availability of commercial testing laboratories accredited by the U.S. Government to provide security evaluation services focused on the needs of both the producers and users of IA products. The standards and methodologies used in the evaluation process are internationally recognized and were developed under terms of the International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement.

What is the purpose of the NIAP Program?

The purpose of the NIAP Program is to evaluate COTS IA and IA-enabled products (e.g., a firewall or an operating system) in accordance with the "International Common Criteria for Information Technology Security Evaluation", generally referred to as the "Common Criteria." The Common Criteria specifies information security functional requirements and seven predefined assurance packages, known as **Evaluated Assurance Levels** (EALs), against which products' functions are tested and evaluated. NSTISSP No. 11 does not require testing against any specific function, nor EAL. The seven EALs provide both the vendor and user with the flexibility to define functional and assurance requirements that are unique to their operating environments and to obtain an evaluated product best suited to those needs. Two very important specification documents are associated with the NIAP Program and the Common Criteria, i.e., **"protection profiles"** and **"security targets**".

*A **protection profile** is the specification document used by a consumer, consumer group, vendor, or any consortium to specify what functional requirements they would like to have in a commercial IA or IA-enabled product, and to document to what assurance level(s) they would like to have the product tested*. Protection profiles for IA and IA-enabled products can be developed by anyone ranging from a commercial producer to an intended government user of those products. NSA and NIST are jointly developing and issuing a series of protection profiles that will address both specific technologies (e.g., firewalls), as well as levels of security robustness. There are three levels of robustness, i.e., Basic, Medium and High. These profiles are being developed under the auspices of

the Information Assurance Technology Framework **(IATF),** a collaborative government and commercial vendor technical initiative.

Protection profiles *serve two purposes:*

a. Provide customers with the ability to specify security requirements for their given environment (levels of concern/robustness); and
b. Serve to identify, for vendors, known markets for products that meet specified customer requirements.

*A **security target** is the specification document that a vendor would use to make security functionality claims about its product.* To have a product evaluated, the vendor must develop a security target. As a part of the security target development process, the vendor can claim conformance to a protection profile, but is not required to do so. The evaluation and testing methodologies are the same for the evaluation of a security target regardless of whether or not it claims conformance to a protection profile. The security requirements in the security target describe the product's security functionality claims, as well as the desired level of evaluation (i.e., the EALs mentioned above) that the vendor desires the NIAP Program laboratory to test against. The objective of the testing is to substantiate vendor claims regarding security functionality at a given assurance level.

What are Protection Profile compliant products?

The difference between products compliant with a protection profile and products that are not compliant is based on a determination as to whose requirements are being met (i.e., is it the vendor's or the customer's). For products claiming compliance to a specific protection profile, the requirements are set and the vendor must include in the product's security target all of the requirements stated in the protection profile. If, during the evaluation, it is determined that the product has difficulty in satisfying a requirement, the vendor must either fix the product, or drop their claim of conformance to the protection profile. For products not claiming compliance to a protection profile, the vendor only has to include in its security target those requirements for which they desire an evaluation. If, during the evaluation, the product has trouble satisfying a particular requirement, the vendor has the option to remove the requirement (i.e., the claim) from the security target and proceed with the evaluation. Products that are compliant with a protection profile provide the consumer with confidence that all of the necessary requirements for the technology operating within the defined level of concern or robustness (e.g., Basic, Medium or High) have been satisfied. For products that do not claim compliance with a protection profile, the consumer must ensure that the security target for this evaluation includes all of the necessary requirements for the particular level of concern or robustness where they plan to use the product.

What is the NIAP Program evaluation process and how does it work?

The NIAP Program evaluation process requires that a vendor first develop and document the security target (described above) which makes security functionality claims

about its product. The next step in the evaluation process is for the vendor to take its security target to one of the NIAP-accredited Common Criteria Testing Laboratories **(CCTLs)** for formal evaluation. The CCTL will evaluate the security target for completeness, consistency and conformance against the requirements of the Common Criteria. Once this is successfully completed, the CCTL will evaluate and validate how the product satisfies its security target. At the conclusion of the evaluation, if the product has satisfied all requirements, NIST and NSA will jointly issue a certificate validating the product's evaluation; place the product on the Validated Products List; and make a Validation Report available to the public.

After a product has successfully completed an evaluation, the vendor has two options for maintaining the validity of the evaluation as the product evolves from one version to the next:

a. Simply request a re-evaluation of the next version of the product, or
b. Participate in the **NIAP Assurance Maintenance Program**.

To participate in the Assurance Maintenance Program, the vendor must include in the initial evaluation request, specific assurance maintenance requirements that address how it plans to maintain the product and a Categorization Report of what will be maintained. As a participant in the assurance maintenance program, a vendor will have to only validate changes to the product and will not be required to go through a completely new evaluation process for each and every product version. All NSA/NIST protection profiles for the federal government will contain requirements for participation in the assurance maintenance program.

What are the advantages of testing in accordance with International Standards?

As noted above, the NIAP Program provides for the evaluation of commercial products in accordance with internationally recognized testing methodologies and standards. *The advantage of this approach* is that commercial vendors (either domestic or foreign) are not limited to having their products tested within their own countries. Any commercial testing laboratory accredited as compliant with the **Common Criteria Mutual Recognition Arrangement (CCMRA)** can perform these evaluations. This arrangement ensures that accredited laboratories, regardless of their geographic location or national affiliation, will test products against the same criteria and use the same testing methodology. The United States, Canada, France, Germany, the Netherlands and the United Kingdom are all charter members of the Common Criteria Recognition Arrangement that was signed in October of 1998. Since that time, Australia, New Zealand, Finland, Greece, Israel, Norway, Spain and Sweden have also become members. Of these nations, the United States, Canada, France, Germany, the United Kingdom and Australia/New Zealand (combined) have programs in place to evaluate COTS IA and IA-enabled products against the Common Criteria. The remaining nations do not have evaluation programs, but have agreed to accept the certificates produced by those nations that do have evaluation programs.

Based on the need for good security products, as well as the plethora of products and services available on the commercial market, consistency and efficiency are desirable objectives. The use of recognized, common standards within the structure of NIAP provides the mechanisms for accomplishing those objective. Specifically,

- The evaluations of IT products and protection profiles are performed against high and consistent standards that are seen as contributing significantly to the confidence in the security of those products and profiles;
- The framework of the Common Criteria increases the availability of evaluated, security-enhanced IT products and profiles for national applications;
- Duplicative evaluations of IT products and protection profiles are eliminated; and
- Continuous improvements in the efficiency and cost-effectiveness of security evaluations and the certification/validation processes for IT products and protection profiles are achieved.

How are the FIPS and CMVP different?

The FIPS evaluation process provides a mechanism for the evaluation of products in accordance with national standards established by NIST. The CMVP is a component of the overall FIPS framework that focuses on the performance of cryptographic modules designed and built to provide confidentiality for sensitive information. *The CMVP provides customers with confidence, accomplished via a functional testing of the product, that commercial cryptographic modules meet one of the four security specification levels* documented in Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, and that the FIPS-approved algorithms are properly implemented. Assurance of the proper functioning of cryptographic modules and algorithms is critical because these modules/algorithms are used to protect sensitive data transmitted over non-trusted paths such as the commercial Internet.

How do NIAP and CMVP function as complementary programs?

Both the NIAP and CMVP programs are intended to evaluate the robustness levels provided by individual COTS IA products. While both programs are used to evaluate robustness levels within COTS IA and IA-enabled products, *they each focus on different aspects of the product and use different criteria.* The CMVP program provides customers with confidences that commercial cryptographic modules meet one of the four security specification levels documented in FIPS 140-2, Security Requirements for Cryptographic Modules, and that the FIPS-approved algorithms are properly implemented. Conversely, the NIAP Program provides consumers with confidences that the non-cryptographic security functions of an IA or IA-enabled product meets one of the seven robustness levels (i.e., EALs) documented in the Common Criteria.

Depending on user applications (e.g., a situation where the only desired security requirement is confidentiality of data), the CMVP program may be sufficient for validating the robustness level of the product and providing the basis for implementation and commencement of operational use. However, in most cases, evaluated COTS IA or

IA-enabled products are often integrated into broader IT systems that address more than one security requirement. For example, tested cryptographic modules are often integrated into other commercial IT products with additional non-cryptographic functionalities. The confidence provided by CMVP testing does not imply an overall confidence with regard to other aspects of the IT product or system into which the module may be integrated. In such cases, a separate NIAP Program evaluation process should be used to complement the CMVP certification process with the objective of ensuring that that the overall system configuration is adequately addressing all of the desired security requirements.

As a general rule, the CMVP program should be viewed as sufficient for the evaluation of products where encryption is the only security requirement, e.g., standalone encryption appliances or Virtual Private Networks (VPNs) where other IA products such as firewalls are not included. Products that integrate basic data encryption with other IA functionalities (e.g., full firewall functionality) require an evaluation of the cryptographic components in accordance with CMVP, as well as the evaluation of other IA system components and the entire system integrity in accordance with the requirements of the NIAP Program.

How should NSTISSP No. 11 be viewed?

NSTISSP No. 11 should be viewed as a tool for evaluating the security functionality provided by COTS IA and IA-enabled products at various robustness levels. A comprehensive risk management program must be considered from the outset in the design, acquisition and operation of all Information Technology (IT) systems. During the initial design phase of any information system, security considerations must be included. Compliance with the policy in its most simplistic form (i.e., feeling comfortable that a properly evaluated product has been acquired), however, should not be viewed as an "end result" IA solution in and by itself. The use of properly evaluated products certainly contributes toward the security and assurance of the overall system where they are employed and should be an important factor in IT procurement decisions. *From an overall security perspective, however, a properly evaluated product is only a part of the security solution. Other complementary controls are needed* including sound operating procedures, adequate training, overall system certification and accreditation, sound security policies and well-designed system architectures.

Why is NSTISSP No. 11 so important?

NSITSSP No. 11 is a critical policy component of the U.S. Government's overall Information Assurance (IA) strategy. A wide variety of products are available to satisfy a diversity of security requirements to include providing confidentiality for data, as well as authenticating the identities of individuals or organizations exchanging sensitive information. In terms of design, quality and performance, these products run the gamut from "terrific-to-terrible". It is imperative that policies and processes be established to validate the performance claims of marketed IA products, and to ensure that these products are responsive to the security needs of the intended users. In the context of

national security systems and information, these requirements take on added significance and importance. NSTISSP No. 11 is a binding, national policy requirement. Acquirers, users and vendors of IA products are encouraged to familiarize themselves with the policy and its associated processes, and to ensure, effective 1 July 2002, full compliance with its documented requirements.

Is there any acquisition guidance available regarding NSTISSP No. 11?

Effective 1 July 2002, U.S. Government Departments and Agencies will be required to acquire, for use on national security systems, only those IA and IA-enabled products that have been evaluated or validated in accordance with the requirements of NSTISSP No. 11, and its associated programs and processes. For FIPS compliant cryptographic modules, products from the NIST CMVP Validation List should be selected. For non-cryptographic module products, the recommended approach is to first choose a product from the NIAP Program (i.e., CCEVS) Validated Products List that is compliant with the requirements of a government-sponsored protection profile for the desired technology (e.g., firewalls). In the absence of any products that are compliant with a government-sponsored protection profile, or where there is no government-sponsored protection profile for that particular technology, the consumer should choose from the Validated Products List an evaluated product from the desired technology that has met its security target requirements. Lastly, where no evaluated or validated product is on the Validated Products List, the consumer should check the NIAP CCEVS Products In-Evaluation List for a potential product.

All proposed contracts for the acquisitions of IA or IA-enable products should contain language that very specifically documents the requirement for NSTISSP No. 11 evaluated/validated products. This can be accomplished in two ways:

a. Where a government-sponsored protection profile exists, the acquisition or contract language should state that the product must be evaluated/validated and be compliant with the requirements of the protection profile; or
b. In the absence of a protection profile, the acquisition or contract language should call for the product to have been evaluated against a consumer-defined set of functions at a given EAL. (At a minimum, products should be certified to EAL2, i.e., basic robustness.)

Where no product exists for a particular technology on the Validated Products List, the acquisition should require, as a condition of purchase, that a vendor submit the product for evaluation in accordance with the requirements of NSTISSP No. 11. Additionally, when a U.S. Government protection profile is developed and released, products of that particular type that are still in development should be evaluated and validated to the new protection profile. Products already in use under this option do not have to be re-evaluated when a protection profile is developed for that product type.

Is it possible to obtain waivers to the requirements of NSTISSP No. 11?

It should be noted that NSTISSP No. 11 does have a provision for waivers. However, the use of waivers is not encouraged, and the waiver process should not be viewed as an "easy way out" for not complying with the requirements of the policy. Where absolutely necessary, waivers should be submitted to the Committee on National Security Systems (CNSS), and they will be reviewed and considered on a case-by-case basis. Government Departments and Agencies desiring to pursue a waiver must enter their request through the Information Assurance Solutions Customer Relations Office at the National Security Agency (NSA). Requests for waivers, including explanatory details, as well as an accompanying justification and rationale, should be forwarded to:

Director, National Security Agency (DIRNSA)
ATTN: V1
STE 6740
Fort George G. Meade, MD 20755-6740

Where can additional information on NSTISSP No. 11 and associated NSA/NIST programs be found?

Additional information on the topics addressed in this memorandum may be found at the following government websites:

- NIST Computer Security Handbook and the Common Criteria:

  http://csrc.nist.gov/nistpubs/ and http://niap.nist.gov/cc-scheme

- International Common Criteria:

  http://www.commoncriteria.org

- NIAP:

  http://niap.nist.gov

- FIPS 140-1 Specifications and Current Validated Modules:

  http://csrc.nist.gov/cryptval/

- NIAP Validated Products List (VPL):

  http://niap.nist.gov/cc-scheme/ValidatedProducts.html

  http://niap.nist.gov/cc-scheme/PPRegistry.html

- Information Assurance Technical Framework (IATF):

  http://www.iatf.net

- NSA/NIST U.S. Government Recommend Protection Profiles:

  http://www.iatf.net